IJAMESC, Vol. 3 No. 01, February 2025
DOI: https://doi.org/10.61990/ijamesc.v3i1.455 e-ISSN 2986-8645

ANALYSIS OF PHARMING IN CYBER CRIME AND ITS IMPACT ON CUSTOMER TRUST (CASE STUDY ON BANK BRI CUSTOMERS BANDAR LAMPUNG REGIONAL OFFICE)

Ranny Caroline[1]*, Tina Miniawati Virgawenda Barusman[2]
[1.2]Faculty of Economics and Business, Bandar Lampung University, Indonesia
*Corresponding Author:
ranny.21021028@student.ubl.ac.id

Abstract
This study aims to determine and analyze the impact of pharming and cybercrime and to disseminate information about factors that affect customer trust in the use of mobile banking, a case study on Bank BRI, Bandar Lampung Regional Office. This study is quantitative research with a sample of 100 respondents, data collected through questionnaires using convenience sampling techniques with hypothesis testing using SmartPLS. The results of this study show that pharming and cybercrime have a positive and significant influence on customer trust. Therefore, it is hoped that financial institutions can commit to improving the security system of mobile banking applications periodically to maintain customer trust. Researchers are further expected to explore the latest techniques of pharming attacks or cybercrime as well as preventive measures that financial institutions can take.

Keywords: Technology, Pharming, Cyber Crime, Mobile Banking, Customer Trust

1. Introduction

Law Number 11 of 2008 concerning Electronic Information and Transactions (UU ITE) is a legal rule in Indonesia that regulates the use of electronic transaction information. The purpose of this law is to provide a legal basis for activities in the digital world, protect the interests of the public, and prevent cybercrime and violations related to information technology. Information technology is a technique in collecting, preparing, storing, processing, announcing, analyzing, and disseminating information.

Technology Internet (IntraConnected Networking) is one of the parts of innovation in technological development that is accelerating (Setiawan & Wahyudi, 2023). Humans assume that the existence of internet, making work and needs met effectively and efficiently (Egan & Prawoto, 2021), and by taking advantage of technological advances, more information is available quickly (Anom et al., 2022). As a result of technological advancements, one way to improve service quality is through the provision of various technology-based services (Pradita & Barusman, 2024). Rapid advancement of technological services internet One of them is in the banking world, namely technology. mobile banking. Mobile banking is the result of technological advancements internet which is used to conduct banking-related transactions. Use Mobile Banking Banking transactions will take place in cyberspace carried out by users without the help of banks. Launch of the BRI application Mobile Banking At the end of February 2019, BRI is one of the banks that uses technological capabilities to improve services to its customers (Desrianto & Noviyanti, 2019).

Risks that arise as a result of increased usage internet due to the actions of technology criminals, which are often referred to as Cyber Crime. (Arofah & Priatnasari, 2020).

Cyber crime take advantage of technological developments. This crime has a big impact on banking because of crime Cyber is a crime committed using technology internet as a tool (tools). Banking crimes aim to obtain account information, credit cards, and hack bank database systems or rob banks (Al Majed et al. 2016; Faridi, 2019).

Pharming is one of the crimes that threatens and traps the victim with the concept of luring the victim (Azzahra et al., 2024; Wibowo & Fatimah, 2017). Attacker sends E-mail Or a message that looks legitimate is from a credit card company or financial institution that asks for account information and often indicates a problem. This research was conducted to improve user customer understanding Mobile Banking about Pharming deep Cyber Crime and emphasizes continuous efforts to protect user customers Mobile Banking from the attack Phraming. Pharming has an impact on the level of trust of BRI bank customers, because the application security is good and guaranteed Mobile Banking provided will increase customer confidence to use the application.

Case Pharming Bank BRI occurred in August 2018 at the BRI Ponorogo branch. Setyo Budiono lost money in his savings account worth Rp 21.5 million without his knowledge. Setyo Budiono gets a notification from the application m-banking who has made four transactions without his knowledge as the account owner (Alawi & Purba, 2019). Pharming against banking also occurred in July 2023, namely a BRI Malang priority customer lost money worth Rp. 1.4 billion within a few hours. F this happened because the victim received a message containing an invitation with an apk format in the application Whatsapp. The victim clicked and opened the invitation and within a few hours the balance in his account was empty (Wulandari, 2023). In mid-October 2023, one of the BRI bank customers in Kudus also lost money worth Rp. 72 million after opening the BRImo application (Hassani, 2024).

The case of savings theft in Palembang through Mobile Banking Ratna Aprianingsih's BRImo is around Rp. 1.4 billion through mobile banking. This incident was due to Ratna clicking Link sent via text message by the perpetrator (Sormin, 2023). Nur, one of the customers of BRI Lampung bank, lost his savings worth Rp 20 million in an instant when he was not using the application m-banking, Nur felt disappointed because the money she had saved in the BRI bank account was stolen by the perpetrators (Nur, 2021). The Tulang Bawang Police, Lampung arrested 12 fraudsters using the fake BRImo website. The perpetrator sent the victim to the site Web fake to drain the victim's savings (Jaya & Purba, 2022).

This study was conducted to analyze the vulnerability of pharming attacks in mobile banking, identify the impact of pharming attacks on customer trust in the digital banking environment, in terms of financial losses and the level of trust in the banking system.

This research has several differences with the research conducted by Darmawan et al., 2023 which are contained in several aspects. The previous study was conducted in 2023, while this study was carried out in 2024, so there are differences in the time context that can affect the results and relevance of the data. Sample collection techniques Convenience sampling, namely a sampling method based on ease of access and availability of respondents, while previous research used the grounded theory through an iterative and theoretical process. In this study, data was collected through a questionnaire with measurements using the Likert scale to evaluate the perception of respondents, while Darmawan's research et al., 2023 uses interview and observation methods, which focus more on the exploration of the direct experience of the research subject.

2. Theoretical Background

2.1 Theory Cyber Security

Schjolberg & Ghernaouti-Helie, (2009) Cyber Security is a mechanism used to protect and prevent intentional and unintentional interference with the confidentiality, integrity, and availability of information. A well-functioning infrastructure determines security. As for according to Silalahi, (2022) In his book, Cyber Security (cybersecurity) an activity of protecting computers, mobile devices, servers, electronic systems, networks, and data from attacks Cyber. The purpose of this effort is to ensure that organizations and institutions in Indonesia have done their duty wisely and carefully to protect the security of their information systems from Cyber around. Cyber security globally based on five areas of work: 1) Legal Certainty (Cybercrime Legality); 2) Technical and action procedural; 3) Organizational Structure; 4) Capacity building and user education; 5) International cooperation.

The goal of cyber security is integrity that allows efforts to reduce the occurrence of serious cyber threats. If cyber threats are a form of cyber crime, they must be faced with careful technical preparation with strategic planning using strategies that are able to overcome problems with cyber threats related to hacking in Indonesia. This shows that cyber security must continue to be improved to prevent cyber crime. In addition, this theory is very relevant to the problem at hand. If a cyber threat occurs, it must be faced with careful technical preparation and strategic planning through strategies to overcome the problem of cyber hacking in Indonesia.

2.2 Mobile Banking

According to Bank Indonesia Regulation Number 19/12/PBI/2017, the development of technology and information systems continues to give birth to various innovations related to technology. The bank has taken advantage of technological advances to provide new banking services, namely Mobile Banking (Nurdin et al., 2020). According to the Financial Services Authority (OJK), Mobile Banking is an electronic banking service that allows customers to make banking transactions using mobile devices or Tablets. Research conducted (Ayuningtyas & Sufina, 2023), one of the bank facilities in the contemporary era that follows the development of technology is banking Mobile. Ease of banking services MobileBanking Mobile is growing rapidly in Indonesia. (Sudaryanti et al., 2019). Mobile banking Improve the efficiency of banking services and facilitate customer transactions (Amalia & Hastriana, 2022).

Occurrence Mobile Banking allows users to make financial transactions, and use various banking services Online via the app or website Web Banking designed specifically for devices Mobile (Darmawan et al., 2023). Mobile banking offers many services, such as fund transfers between banks and other banks, information on balances and mutations, bill payments, such as installments, insurance, electricity, water, and telephone, and more (Antonov et al., 2022; Dwinurpitasari, 2019). The service is available in the bank's official application which can be used anytime and anywhere. Customers are more interested in using Mobile Banking because they have digital skills, sufficient literacy, have access to internet and supporting digital devices (Naeem & Ozuem, 2021).

2.3 Cyber Crime

Technological developments that continue to advance, Cyber Crime remains a rapidly evolving threat, and protection against attacks Cyber is one of the top priorities for governments and organizations around the world. Cyber crime is a crime committed in a

Online. According to Law No. 11 of 2008 which was amended into Law No. 19 of 2016 concerning Information and Electronic Transactions, Cyber Crime is a criminal act related to prohibited activities, disturbances (interferens), supporting prohibited acts, and falsifying information or electronic documents. These crimes do not choose time and target, and can happen to anyone and anywhere (Vest & Muaja, 2021). Cyber crime, or world evil, is the most common crime in the technological world by using the internet as a tool.

However, these crimes are not directly visible and do not cause physical injury, Cyber Crime cause serious harm, such as thieves who can steal important data that can be misused (Amanda Fitria Najwa et al., 2024). Cyber crime It involves the use of computers in its implementation. Practice Cyber Crime done by an individual or a group of people who are experts in hacking (Vest & Muaja, 2021). Cyber Crime covering various types of crimes including hacking, phishing or pharming, malware, ransomware, identity theft, cyberstalking, carding, DDoS attack (Distributed Denial of Service), spamming, online fraud, data breach, social engineering.

2.4 Pharming

Large number of users internet around the world, causing Hackers to seek benefits from the use of internet. Pharming is a form of criminal attack Cyber that aims to divert traffic internet users to the site website by manipulating the DNS system (Domain Name System) or change the settings file hosts on the user's computer by impersonating a trusted institution to obtain sensitive customer data information (Darmawan et al., 2023). Pharming and phishing almost the same, Hackers using malicious systems such as user devices or DNS servers to redirect users to unauthorized sites (Lallie et al., 2021). Pharming is a development of phishing, but more sophisticated because these attacks can occur even if the user types in the site Web which is true.

Pharming done by utilizing DNS as the main weapon, while phishing Using the Site Web fake that appears legitimate to the user internet. Hackers Using the attack Pharming to encourage people to visit your site Web fake, calling fake phone numbers, or downloading malicious software to steal personal information such as account numbers, credentials Login, credit card number, password, or PIN (Azeez et al., 2022). This case is very detrimental to the victim materially because Hackers taking the savings account of the customer who was the victim. Pharming is a serious threat because it is difficult for ordinary users to detect. Users can feel safe when accessing sites that look genuine, but are actually victims of attacks targeted to steal data. In addition, the impact that occurred as a result of the attack Pharming is a loss of customer trust. Customer trust is fundamental in dangerous situations, and mobile apps have a variety of vulnerabilities that leave customers vulnerable to various risks (Purwanto et al., 2020). Customer trust is a person's confidence in others in conducting transactions through the internet network based on the belief that the person or company he trusts will fulfill all his obligations properly as expected (Alamsyah & Anugrah, 2015). Attack Pharming causing customers to worry about using Mobile Banking.

Research conducted Darmawan et al., (2023) Demonstrate practice Pharming in crime Cyber has a significant impact on service users Mobile Banking. Better awareness and understanding of Pharming It is essential to protect users from greater losses. Meanwhile, the results of the study Arofah & Priatnasari, (2020) shows that internet banking has a positive and significant effect on cybercrime. It also shows that Cyber Crime new in the

field of banking began to emerge by using increasingly sophisticated applications than conventional methods.

2.5 Frame Mind

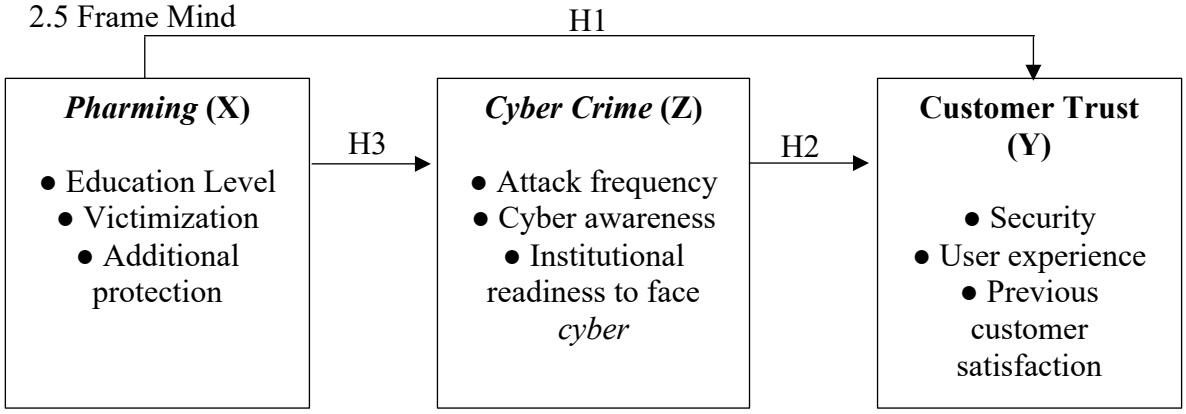

Figure 1. Conceptual Framework (Intercession, 2020)

2.6 Hypothesis

1) H1: Pharming has a direct effect on customer trust
   Pharming is a cybercrime that aims to redirect users' internet traffic to fake websites by manipulating the DNS system. When a bank's mobile banking experiences a pharming crime , customer confidence in mobile banking will decrease. So the higher the pharming attack , the more worried customers will be to use mobile banking and have an impact on decreasing customer confidence.
2) H2: Cyber Crime Has a Direct Effect on Customer Trust
   Cyber crime is a form of crime Online that occur in cyberspace with illegal activities, disturbances, violations that encourage illegal acts, and violations that falsify information or electronic documents. The higher the rate of cybercrime that occurs in Mobile Banking a bank, it will cause a decrease in the use of Mobile Banking which is caused by a decrease in customer trust. According to research Fitri, (2021) Cyber Crime Affects customer trust in the use of Internet Banking, if the security system does not contain crime, then the level of trust will increase and vice versa.
3) H3: Pharming Affects Customer Trust Through Cyber Crime
   Pharming can reduce customer trust through cyber crime because pharming is a part or type of cybercrime. This problem is very detrimental to the victim materially because the hacker took the savings of the customer's account that was the victim so that the customer no longer trusted to use mobile banking

3. Methods

This study uses a type of quantitative data using a scale likert based on primary data sources using questionnaires. Scale likert is a research measurement used to measure respondents' opinions (Sugiyono, 2013). Scale usage likert We can measure the variable value for each question and present it to the respondents as seen in the table below:

Table 1. Likert Scale

Choice of Answer	SS (Strongly Agree)	S (Agreed)	N (Neutral)	TS (disagree)	STS (Strongly disagree)
Value Statement	5	4	3	2	1

(Sugiyono, 2013)

The population in this study is customers of Bank BRI Bandar Lampung Regional Office with the Convenience sampling. Convenience Sampling is a sampling technique based on the ease of the researcher finding respondents who meet the researcher's criteria (Howitt & Cramer, 2011). Sampling was carried out with the formula lemeshow i.e. is a formula used to find the minimum number of samples from an unlimited population (infinite population). Formula lemeshow (Hosmer et al., 1997):

$$n = \frac{z^2.P(1-P)}{d^2}$$

Information:
n = number of samples
z = z score at 95% confidence (1.96)
P = maximum estimate (0.5)
d = sampling error (10%)

The calculation using the lemeshow formula is rounded for the following conformity:

$$n = \frac{1{,}96^2.0{,}5(1-0{,}5)}{0{,}1^2}$$

$$n = 96{,}04 \text{ rounded to } 100$$

The data collection of this research was carried out by distributing questionnaires through Google Form based on the criteria of respondents who are BRImo users in Bandar Lampung, women or men, working or not working, age over 17 years old. This research technique uses the application of data SmartPLS with the SEM method (Structural Equation Modeling) as an analysis that combines the structural model analysis approach (inner model) and measurement model (outer model) (Ghozali, 2016).

4. Results and Discussion

The PLS model is carried out by evaluating the inner and outer models to assess the validity and reliability of the model and to predict the relationships between variables. Evaluation of the model by looking at statistically significant values to determine the influence between variables first, the form of the inner and outer model design path diagram in the study is as follows:

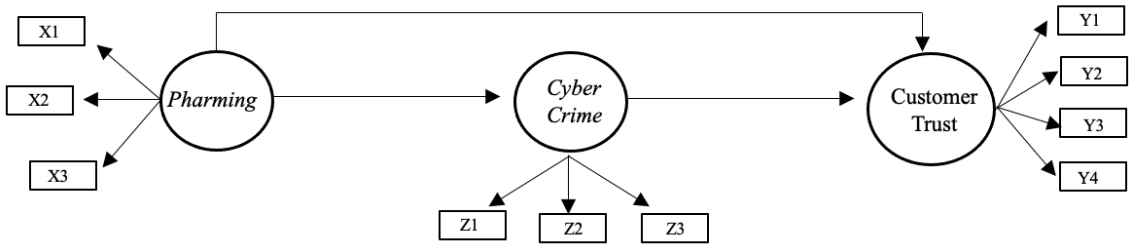

Figure 2. Model Test Results
Source: Data processed (2024)

The criteria for data analysis with SmartPLS 4.0 in assessing the outer model can be done by looking at convergent validity, discriminatory validity, composite reliability, and cronbach's alpha. Meanwhile, to assess the inner model by bootstrapping, t-statistical test parameters were obtained to predict the existence of causality relationships.

Table 2. Test Results of Outer Loading, Cornbach's A, Composite R, AVE

Variable	Indicators	Outer Loading	Cronbach's Alpha	Composite Reliability	AVE
Pharming	X1	0,776	0,672	0,676	0,602

DOI: https://doi.org/10.61990/ijamesc.v3i1.455 e-ISSN 2986-8645

	X2	0,754			
	X3	0,787			
Cyber crime	Z1	0,969	0,743	0,742	0,566
	Z2	0,702			
	Z3	0,969			
Customer Trust	Y1	0,718	0,858	0,906	0,790
	Y2	0,758			
	Y3	0,798			
	Y4	0,732			

Source: Data processed (2024)

The results of data processing through SmartPLS 4.0 outer loading >0.7 is declared valid or meets the requirements of convergent validity between each Items Measurement (indicator) (Irwan & Adam, 2020). Based on the results of data processing, it was found that the value outer loading the table shows the number >0.7. Each indicator is said to have met the requirements of the convergent validity test in the category of both in measuring research variables and valid for use in measuring research variables.

According to Hair et al., (2017) A variable is said to be tested or reliable if it has a value of Cronbach's Alpha >0.7 but in the exploration research the value of Cronbach's Alpha 0.6 – 0.7 is still acceptable. Cronbach's alpha strengthens the reliability test of the consistency of each answer tested. The results of data processing, in the table above each variable has a value of >0.6 and can be said to be reliable.

The AVE score is an additional tool that can be used to test the validity of a crime. A measurement model with AVE is a model that compares the roots of AVE with correlations between constructs. If the root value of AVE >0.5, then the validity discrimination is achieved. The AVE value of each variable in the table is >0.5, so it can be said to be tested or reliable.

Table 3. R-Squared Results

Variable	R-Square	Adjusted R Square
Customer Trust	0,542	0,533
Cyber crime	0,338	0,331

Source: Data processed (2024)

If the value of R-Square >0.67 can be said to be strong, >0.33 moderate and >0.19 weak (Chin, 1998). The table above shows the R-Square for customer trust of 0.542 or 54.2% (moderate) influence Pharming on customer trust and 0.486 or 46.8% are influenced by other factors as well as on the variable Cyber Crime has a value of 0.338 or 38.8% (weak) influence cybercrime on customer trust and the remaining 0.622 or 62.2% were influenced by other factors.

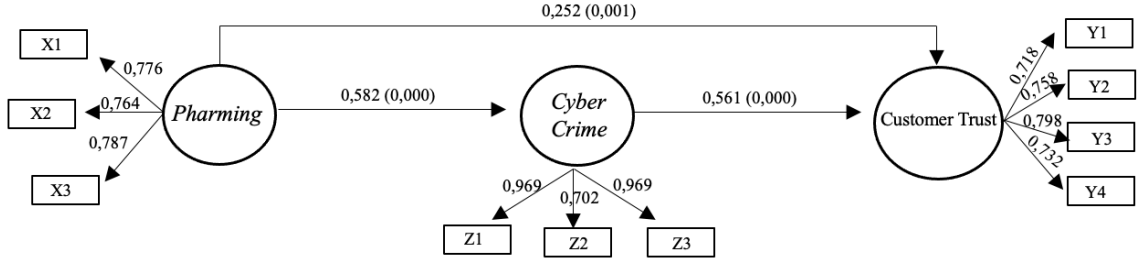

Figure 3. Test Results of Bootstrapping Structural Model (SEM-PLS Graphic Output)
Source: Data processed (2024)

Table 4. Direct Hypothesis Test Results

Relationship between Variables	Original Sample	T-Statistic	P-Value
Pharming → Customer Trust	0,252	3,269	0,001
Pharming → Cyber crime	0,582	8,046	0,000
Cyber crime → Customer Trust	0,561	7,864	0,000

Source: Data processed (2024)

Table 5. Results of Indirect Hypothesis Test

Relationship Between Variables	Original Sample	T- Statistic	P-Value
Pharming → Cyber crime → Customer Trust	0,326	5,493	0,000

Source: Data processed (2024)

Based on calculations bootstrapping above, to find out the significance of the relationship between constructs indicated by the value of t-Statistics, is said to be significant if the value t-statistic >1.96 (Ghozali, 2016) and p-value <0.005.

1) Pharming has a direct effect on customer trust
   The results showed that H1 was accepted with a significant influence Pharming to the decrease in customer trust with the amount of direct relationship of 0.252 and p-value 0.001. When Pharming increases, the level of customer trust will decrease. The amount of t-Statistics on the influence of Pharming 3,269>1.96. The results indicate that significantly the variable Pharming affect the level of customer trust. This research is in accordance with what was conducted by Darmawan et al., (2023) Demonstrate practice Pharming in crime Cyber has a significant impact on service users Mobile Banking. At the time of Mobile Banking A bank is under attack Pharming then the customer's trust will Mobile Banking will experience a decrease because customers are afraid that they will be victims of attacks Pharming which causes financial losses.
2) Cyber Crime Has a Direct Effect on Customer Trust
   The results showed that H2 was accepted with a significant influence Cyber Crime against the level of decline in customer trust with the amount of direct relationship 0.582 and p-value 0.000. When Cyber Crime will decrease customer trust. The amount of t-Statistics on the influence of Cyber Crime 8,046>1.96. The results indicate that significantly the variable Cyber Crime affect the level of customer trust. This research is in line with the research carried out Fitri, (2021) Cyber Crime affect customer trust to use Internet Banking, if the security system does not contain crime, the level of trust is increasing.
3) Pharming Affects Customer Trust Through Cyber Crime
   The results of the study showed that H3 was accepted with the influence of pharming through cyber crime, causing a decrease in customer trust with an indirect relationship of 0.326 and a p-value of 0.000. The t-statistic on the effect of pharming through cyber crime was 5,439>1.96. These results indicate that significantly the pharming variable on the level of customer trust through cyber crime is influential. When pharming increases, cyber crime will also increase, which will cause a decrease in customer confidence to use mobile banking. If pharming increases, the level of cyber crime automatically increases, which causes a decrease in the level of customer confidence in using mobile banking because they are worried and afraid of experiencing financial losses due to cybercrime that occurs.

5. Conclusion

Based on the results of the research and data processing, the researcher concluded that pharming attacks have a significant positive influence on the decrease in customer trust levels with a t-statistic on the influence of pharming 3.269>1.96. Cyber crime also had a positive and significant effect on decreasing the level of customer trust in the t-statistic amount on the influence of cyber crime 8,046>1.96. And pharming has a significant indirect effect on customer trust through cyber crime with the amount of t-statistic on the influence of pharming through cyber crime 5,439>1.96. When pharming increases, cyber crime will also increase, which will cause the level of customer trust to use mobile banking decreases. Customer trust is very important for financial institutions, so it is necessary to increase customer trust by improving the quality of mobile banking services and security.

Financial institutions are expected to improve the security system of applications in mobile banking (BRImo) from cybercrime attacks so that customer trust is maintained. The security of mobile banking services should be a top priority when building mobile banking services. In order to avoid pharming attacks on mobile banking services, users need to implement appropriate security measures, such as using official mobile banking applications downloaded from trusted sources. Financial institutions are also advised to be more transparent in presenting data related to the number of mobile banking service users in their financial reports so that researchers can access information that is easier for researchers, for example through the publication of statistics on mobile banking use on a regular basis. This step not only supports the development of quality academic research, but also helps financial institutions understand their usage trends and increase public trust in the digital services provided.

References

Al Majed, N., Maglaras, L. A., Siewe, F., Janicke, H., & Bagheri Zadeh, P. (2016). Prevention of crime in B2C E-Commerce: How E-Retailers/Banks protect themselves from Criminal Sctivities. ICST Transactions on Security and Safety, 3(7), 151727. https://doi.org/10.4108/eai.8-12-2016.151727

Alamsyah, D. P., & Anugrah, R. (2015). Membangun Kepercayaan Nasabah Pada Internet Banking. Ecodemica, 3(2), 464–473. http://ejournal.bsi.ac.id/ejurnal/index.php/ecodemica/article/view/33

Alawi, M. Al, & Purba, D. O. (2019). Uang di Rekening Bank Milik Pejabat Ponorogo Tiba-tiba Raib, Ini Kronologinya. Kompas. https://regional.kompas.com/read/2019/08/16/20212811/uang-di-rekening-bank-milik-pejabat-ponorogo-tiba-tiba-raib-ini-kronologinya?page=all#page2

Amalia, P., & Hastriana, A. Z. (2022). Pengaruh Kemanfaatan, Kemudahan Keamanan, dan Fitur M-Banking terhadap Kepuasan Nasabah dalam Bertransaksi pada Bank Syariah Indonesia (Studi Kasus BSI KCP Sumenep). Islamic Sciences, Sumenep, 1, 70–89.

Amanda Fitria Najwa, Aqila Husna, & Aqila Husna. (2024). Efektifitas Yurisdiksi Cybercrime di Tengah Perkembangan Teknologi Informasi. Jurnal Hukum Dan Sosial Politik, 2(3), 126–135. https://doi.org/10.59581/jhsp-widyakarya.v2i3.3426

Anom, R. I. P., Barusman, T. M., Barusman, A. R. P., & Wrganegara, T. L. W. (2022). Pengaruh Tingkat Literasi Digital dan Kualitas Teknologi Informasi terhadap Keputusan Berkunjung Turis ke Wisata Bahari Lampung pada masa Pandemi Covid-19. Visionist, 11(2), 15–25.

Antonov, M. P. I., Hassan, F. Z., & Nurisnaini, N. (2022). Pengaruh Mobile Banking Terhadap Kepuasan Nasabah. Jurnal Informatika Kesatuan, 2(2), 189–198. https://doi.org/10.37641/jikes.v2i2.1458

Arofah, N. R., & Priatnasari, Y. (2020). Internet Banking Dan Cyber Crime : Sebuah Studi Kasus Di Perbankan Nasional. Jurnal Pendidikan Akuntansi Indonesia, 18(2), 107–119. https://doi.org/10.21831/jpai.v18i2.35872

Ayuningtyas, M., & Sufina, L. (2023). Pengaruh Penggunaan Mobile Banking, Internet Banking, dan Atm terhadap Kinerja Keuangan Perbankan (Studi Kasus Sektor Bank Konvensional yang Terdaftar di Bursa Efek Indonesia) Tahun 2017- 2021. Jurnal Keuangan Dan Perbankan, 19(2), 119–130. https://doi.org/10.35384/jkp.v19i2.394

Azeez, N. A., Oladele, S. S., & Ologe, O. (2022). Identification of Pharming in Communication Networks using Ensemble Learning. Nigerian Journal of Technological Development, 19(2), 172–180. https://doi.org/10.4314/njtd.v19i2.10

Azzahra, N. S., Tambunan, A. M., Aulia, N. N., Binarsih, A., & Saepudin, T. H. (2024). Tinjauan Literatur Tentang Ancaman Cybercrime dan Implementasi Keamanan Siber Di Industri Perbankan . HUMANITIS: Jurnal Humaniora, Sosial Dan Bisnis, 2(7), 692–700.

Chin, W. W. (1998). The Partial Least Squares Aproach to Structural Equation Modeling. Modern Methods for Business Research. 8.

Darmawan, I., Sutarsih, S. R., Hasanah, U., Riyan, & Firdaus, A. (2023). Analisis Pharming Dalam Cyber Crime di Layanan Mobile Banking. Jurnal Informasi Dan Teknologi, 5(2), 159–163. https://doi.org/10.37034/jidt.v5i2.362

Desrianto, M., & Noviyanti, S. (2019). Luncurkan BRImo, Strategi BRI Gaet Millenial. Kompas.Com. https://money.kompas.com/read/2019/02/28/075018326/luncurkan-brimo-strategi-bri-gaet-millenial#

Dwinurpitasari, Y. A. (2019). Pengaruh Kualitas Layanan dan Produk Mobile Banking Terhadap Kepuasan Nasabah pada BRI Syariah KCP Ponorogo. 1–23.

Egan, R., & Prawoto, H. (2021). Pengaruh Internet Banking Terhadap Kinerja Perbankan di Indonesia (Studi Empiris Pada Bank Yang Listing Di BEI). Jurnal Akuntansi Bisnis, 11(22), 138–153.

Faridi, M. K. (2019). Kejahatan Siber Dalam Bidang Perbankan. Cyber Security Dan Forensik Digital, 1(2), 57–61. https://doi.org/10.14421/csecurity.2018.1.2.1373

Fitri, J. (2021). Pengaruh Internet Banking dan Cyber Crime Terhadap Kepercayaan Nasabah di Perbankan Syariah.

Ghozali, I. (2016). Aplikasi Analisis Multivariete SPSS 23 (8th ed.). Badan Penerbit Universitas Diponegoro.

Hair, J. F., Hult, G. T., Ringle, C., & Sarstedt, M. (2017). A Primer on Partial Least Squares Structural Equation Modeling (PLS-SEM) - Joseph F. Hair, Jr., G. Tomas M. Hult, Christian Ringle, Marko Sarstedt. In Sage.

Hassani, N. (2024). Kronologi Saldo Rp 72 Juta Nasabah di Pecangaan Jepara Raib Usai Login BRImo, Hingga Gugat Keamanan Aplikasi. Radar Kudus. https://radarkudus.jawapos.com/jepara/693695910/kronologi-saldo-rp-72-juta-nasabah-di-pecangaan-jepara-raib-usai-login-brimo-hingga-gugat-keamanan-aplikasi

Hosmer, D. W., Hosmer, T., Le Cessie, S., & Lemeshow, S. (1997). A comparison of goodness-of-fit tests for the logistic regression model. Statistics in Medicine, 16(9), 965–980. https://doi.org/10.1002/(SICI)1097-0258(19970515)16:9<965::AID-SIM509>3.0.CO;2-O

Howitt, D., & Cramer, and D. (2011). Introduction to Research Methods in Psychology (thrid). Pearson Education Limited.

Irwan, & Adam, K. (2020). Metode Partial Least Square (Pls) dan Terapannya. Teknosains, 9(1), 53–68.

Jaya, T. P., & Purba, D. O. (2022). Hati-Hati Penipuan Berkedok Kenaikan Tarif Transfer BRI, Dikirimi Link BRImo Palsu lalu Uang Anda Lenyap. Kompas.Com. https://regional.kompas.com/read/2022/11/11/145617078/hati-hati-penipuan-berkedok-kenaikan-tarif-transfer-bri-dikirimi-link-brimo

Lallie, H. S., Shepherd, L. A., Nurse, J. R. C., Erola, A., Epiphaniou, G., Maple, C., & Bellekens, X. (2021). Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic.

Naeem, M., & Ozuem, W. (2021). The role of social media in internet banking transition during COVID-19 pandemic: Using multiple methods and sources in qualitative research. Journal of Retailing and Consumer Services, 60(February), 102483. https://doi.org/10.1016/j.jretconser.2021.102483

Nur. (2021). Hilangnya Saldo Puluhan Juta Rupiah di Rekening Bank BRI. Media Konsumen. https://mediakonsumen.com/2021/11/03/surat-pembaca/hilangnya-saldo-puluhan-juta-rupiah-di-rekening-bank-bri

Nurdin, N., Musyawarah, I., Nurfitriani, N., & Jalil, A. (2020). Pengaruh Pelayanan Mobile Banking Terhadap Kepuasan Nasabah (Studi Pada Mahasiswa Perbankan Syariah IAIN Palu). Jurnal Ilmu Perbankan Dan Keuangan Syariah, 2(1), 87–104. https://doi.org/10.24239/jipsya.v2i1.24.87-104

Pradita, S., & Barusman, M. Y. S. (2024). The Effect of Service Quality and Service Innovation on Customer Satisfaction at PT PLN (Persero) ULP Teluk Betung. Formosa Journal of Multidisciplinary Research, 3(3), 65–80. https://doi.org/10.55927/fjmr.v3i3.8559

Purwanto, E., Deviny, J., & Mutahar, A. M. (2020). The Mediating Role of Trust in the Relationship between Corporate Image, Security, Word of Mouth and Loyalty in M-Banking Using among the Millennial Generation in Indonesia. Management and Marketing, 15(2), 255–274. https://doi.org/10.2478/mmcks-2020-0016

Rompi, T., & Muaja, H. S. (2021). Tindak Kejahatan Siber di Sektor Jasa Keuangan Dan Perbankan. Lex Privatum, 9(4), 183–192. https://ejournal.unsrat.ac.id/index.php/lexprivatum/article/view/33358

Schjolberg, S., & Ghernaouti-Helie, S. (2009). A Global Protocol on Cybersecurity and Cybercrime. E-dit.

Setiawan, N., & Wahyudi, I. (2023). Pencegahan fraud pada kejahatan siber perbankan. Kabilah: Journal of Social Community, 8(1), 508–518.

Silalahi, F. D. (2022). Cyber Security (J. T. Santoso (ed.)). Yayasan Prima Agus.

Sormin, A. (2023). Jangan Buka Link Undangan APK, Honorer ini Kuras Tabungan Korban Rp1,4 Miliar Lewat Brimo. Lampungpro.Co. https://lampungpro.co/news/jangan-buka-link-undangan-apk-honorer-ini-kuras-tabungan-korban-rp14-miliar-lewat-brimo

Sudaryanti, D. S., Sahroni, N., & Kurniawati, A. (2019). Analisa Pengaruh Mobile Banking Terhadap Kinerja Perusahaan Sektor Perbankan Yang Tercatat di Bursa Efek Indonesia. Jurnal Ekonomi Manajemen, 4(2), 96–107. https://doi.org/10.37058/jem.v4i2.699

Sugiyono. (2013). Metode Penelitian Kuantitatif Kualitatif dan R&D. Alfabeta Bandung.

Syafaati, F. (2020). Pengaruh Kepercayan dan Mutu e-banking terhdap Minat

Bertranskasi Secara Online dan Dampaknya Pada Keputusan Nasabah Dalam Bertransaksi Secara Online (Studi Pada Nasabah Bank Negara Indonesia Syariah di DKI Jakarta). In Skripsi.

Wibowo, M. H., & Fatimah, N. (2017). Ancaman Phishing Terhadap Pengguna Sosial Media Dalam Dunia Cyber Crime. JOEICT(Jurnal of Education and Information Communication Technology), 1(1), 1–5. https://www.jurnal.stkippgritulungagung.ac.id/index.php/joeict/article/view/69

Wulandari, F. (2023). Jadi Korban Phising, Saldo Nasabah BRI Malang Ini Raib Rp 1,4 Miliar. Tribun News. https://www.tribunnews.com/regional/2023/07/09/jadi-korban-phising-saldo-nasabah-bri-malang-ini-raib-rp-14-miliar#google_vignette